last worksheet:

$R = \mathbb{Z}[\sqrt{-5}]$ $\qquad\qquad$ $(1+\sqrt{-5})(1-\sqrt{-5}) = 6$

$I = (2, 1+\sqrt{-5})$

$J = (3, 1+\sqrt{-5})$

$K = (3, 1-\sqrt{-5})$

$J \cdot K = \langle 3 \rangle$

by def, $J \cdot K = \{ \underline{a_1 b_1} + \dots + a_k b_k \mid a\text{'s} \in J,\ b\text{'s} \in K \}$

gen. elt. of J looks like $3x + (1+\sqrt{-5})y$ where $x, y \in R$

— — K —— $3z + (1-\sqrt{-5})w$ where $z, w \in R$

product is $\underline{3}xz + \underline{3}(1-\sqrt{-5})xw + \underline{3}(1+\sqrt{-5})yz + \underline{6}yw$

it's a multiple of 3.

any sum of these is a mult. of 3

so $\underline{J \cdot K \subset \langle 3 \rangle}$

OTOH, $3 \cdot 3 = 9 \in J \cdot K$

$(1+\sqrt{-5})(1-\sqrt{-5}) = 6 \in J \cdot K$

so $9 - 6 = 3 \in J \cdot K$

so $\underline{\langle 3 \rangle \subset J \cdot K}$

so $J \cdot K = \langle 3 \rangle$.

$R = \mathbb{Z}[\sqrt{-5}]$
$I = (2, 1+\sqrt{-5})$
$J = (3, 1+\sqrt{-5})$
$K = (3, 1-\sqrt{-5})$

similar: $I \cdot I = \langle 2 \rangle$
$I \cdot J = \langle 1+\sqrt{-5} \rangle$
$I \cdot K = \langle 1-\sqrt{-5} \rangle$

as promised, this takes failure of unique factorization in R

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

and clarifies it:

$$\langle 6 \rangle = (I \cdot I) \cdot (J \cdot K) = (I \cdot J) \cdot (I \cdot K)$$

beginning of a part of # thy called "class field theory"

one more point: $3 \in J \cdot K$
but 3 can only factor as $3 \cdot 1$ or $(-3)(-1)$

and ± 1 are not in J or K (not obvious?)

so we really needed that clunky sum in the def. of $J \cdot K$.

$R = \mathbb{Z}[\sqrt{-5}]$
$I = (2, 1+\sqrt{-5})$
$J = (3, 1+\sqrt{-5})$
$K = (3, 1-\sqrt{-5})$

while we're here,

$I + J = \langle 1 \rangle$

why? $-2 \in I$, $3 \in J$, so $3 - 2 = 1$ is in $I+J$

so $\langle 1 \rangle \subset I + J$
but $\langle 1 \rangle$ = whole of R
so $I + J = \langle 1 \rangle$

$I + K = \langle 1 \rangle$

$J + K = \langle 1 \rangle$

because $(1+\sqrt{-5}) + (1-\sqrt{-5}) = 2$ is in $I + J$
so $3 - 2 = 1$ is in $I + J$.

we've seen that $\langle 6 \rangle + \langle 10 \rangle = \langle 2 \rangle$ in $\mathbb{Z}$
and $\langle 6 \rangle + \langle 11 \rangle = \langle 1 \rangle$
bec $\gcd(6, 11) = 1$

in example above, I and J are ideals, not numbers

but we should consider them rel. prime because $I + J = \langle 1 \rangle$.

Back to generalities.

R = comm. ring

$I, J \subset R$ ideals

generalizes the fact that $\mathrm{lcm}(m,n)$ divides $m \cdot n$

Prop: $I \cdot J \subset I \cap J$

Pf: gen elt. of $I \cdot J$ looks like

$a_1 b_1 + \dots + a_k b_k$ where $a_i \in I$, $b_i \in J$

each $a_i b_i \in I$ bec. $a_i \in I$ and I is an ideal

and $a_i b_i \in J$ bec. $b_i \in J$ and J is an ideal

so $a_i b_i \in I \cap J$ and so is a sum of $a_i b_i$'s ☒

Could be strictly contained:

in $\mathbb{Z}$, $\langle 6 \rangle \cdot \langle 10 \rangle = \langle 60 \rangle$ but $\langle 6 \rangle \cap \langle 10 \rangle = \langle 30 \rangle$

so $\langle 60 \rangle \subsetneq \langle 30 \rangle$.

Prop: If $I + J = \langle 1 \rangle$ then $I \cdot J = I \cap J$

If $\gcd(m,n) = 1$ then $\mathrm{lcm}(m,n) = mn$

Proof Just need to show that $I \cap J \subset IJ$.

since $I + J = \langle 1 \rangle$, we can write $1 = a + b$ for some $a \in I$, $b \in J$.

given any $c \in I \cap J$, get

$c = \underset{\text{in } I}{a}\underset{\text{in } J}{c} + \underset{\text{in } J}{b}\underset{\text{in } I}{c} \in I \cdot J$ thus $I \cap J \subset I \cdot J$ ☒